Advisory 2019-08

Security update for CODESYS Control V3 password handling

Published: 29 March 2021

Version: 7.0
Template: templ_tecdoc_en_V3.0.docx
File name: Advisory2019-08_CDS-62813.docx

CONTENT

1 Affected Products

All variants of the following CODESYS V3 products in all versions prior V3.5.16.0 containing the CmpUserMgr component are affected, regardless of the CPU type or operating system:
• CODESYS Control for BeagleBone
• CODESYS Control for emPC-A/iMX6
• CODESYS Control for IOT2000
• CODESYS Control for Linux
• CODESYS Control for PLCnext
• CODESYS Control for PFC100
• CODESYS Control for PFC200
• CODESYS Control for Raspberry Pi
• CODESYS Control RTE V3
• CODESYS Control RTE V3 (for Beckhoff CX)
• CODESYS Control Win V3 (also part of the CODESYS Development System setup)
• CODESYS V3 Simulation Runtime (part of the CODESYS Development System)
• CODESYS Control V3 Runtime System Toolkit
• CODESYS HMI V3

To use the new password transport mechanism, also the CODESYS communication clients have to be updated to version V3.5.16.0 or higher:
• CODESYS V3 Development System
• CODESYS Edge Gateway V3
• CODESYS OPC Server V3
• CODESYS PLCHandler SDK

2 Vulnerability overview

2.1 Type

Insufficiently protected credentials

2.2 Management Summary

User credentials are insufficiently protected by the online user management of the CODESYS Control runtime systems.

2.3 References

CVE: CVE-2019-9011, CVE-2019-9013, CVE-2020-6081, CVE-2020-12067, CVE-2020-12069 [6]

ICS-CERT: ICSA-19-213-04 [8]

CODESYS JIRA: CDS-62813, CDS-62814, CDS-64207, CDS-64209, CDS-65129, CDS-65675, CDS-73742

2.4 Severity Rating

3S-Smart Software Solutions GmbH has rated this vulnerability as high.

The CVSS v3.0 base score of 8.8 has been assigned. The CVSS vector string is (CVSS:3.0/AV:A/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:H). [7]

3 Vulnerability details

3.1 Detailed Description

The CODESYS Control runtime system enables embedded or PC-based devices to be a programmable industrial controller and provides several security features to secure the devices. To limit the access to the programming port, it allows defining users with individual passwords or also to configure a role based user management with graded access rights and multiple users. These user credentials are insufficiently protected by the online user management of the CODESYS Control runtime systems.

In detail this advisory comprises the following vulnerabilities:

CVE-2019-9011: Observable response discrepancy
Based on the communication responses of the CODESYS Control runtime system an attacker may be able to enumerate valid users names.

CVE-2019-9013: Insufficiently protected credentials on transport
Without using the TLS based encrypted CODESYS online communication, the user credentials are insufficiently protected on transport.

CVE-2020-12067: Unverified password change
When setting a new password for a user, the CODESYS Control runtime system does not ask for the original password.

CVE-2020-12069: Use of password hash with insufficient computational effort
The CODESYS Control runtime system stores the online communication passwords using a weak hashing algorithm.

CVE-2020-6081: Remote code execution
In order to implement a programmable logic controller, the CODESYS Control runtime system allows code downloading and execution. An attacker could utilize this PLC functionality for malicious purposes if access to the PLC is not secured by the online user management of the CODESYS Control runtime system.

3.2 Exploitability

To exploit these vulnerabilities, an attacker needs access to the online communication traffic or local access to the PLC.

3.3 Difficulty

An attacker with low skills would be able to exploit these vulnerabilities.

3.4 Existence of exploit

No known public exploits specifically target these vulnerabilities, but we are aware of some publicly available information that would allow an exploit to occur.

4 Available software updates

3S-Smart Software Solutions GmbH has released version V3.5.16.0 to solve the noted vulnerability issue for all affected CODESYS products.

Please visit the CODESYS update area for more information on how to obtain the software update [3].

With CODESYS V3.5.16.0, the online user management of the CODESYS Control runtime system has been redesigned. Many parts have been implemented in a compatible way, but it was necessary to do some incompatible changes for security reasons:

• All CODESYS communication clients with a version V3.5.16.0 or higher still support all online features of new and old CODESYS runtime systems. In opposite to that, clients before version V3.5.16.0 can still login and communicate with CODESYS runtime systems with a version V3.5.16.0 or higher, but are not able anymore to modify the online user management on the PLC device. This limitation includes user, password, group and access right modifications.

• On initial startup, an updated CODESYS Control runtime system converts the older user management database into the new format, which is incompatible to the old one. To prepare a later downgrade of the CODESYS Control runtime system to a version before V3.5.16.0, we recommend to backing up the user management before updating to version V3.5.16.0. For this purpose the user management can be saved by the CODESYS Development System in a *.dum file and restored again after downgrading to a version before V3.5.16.0.

• Since version V3.5.16.0, user names, group names and passwords are limited to a maximum of 59 characters. Existing user management configurations that exceed this limit cannot be successfully converted by the

CODESYS Control runtime system.

• For CODESYS Control runtime system version V3.5.16.0, it is not possible anymore to rename user groups.

• Up to version V3.5.16.0, there was a default user "Administrator" with a default password. When activating the user management, you had to log in with these user data and then change the password. With version V3.5 16.0 this default user was removed. To activate the user management, a new user with a freely selectable user name and password must be created. This first user automatically gets administrator rights.

• For CODESYS Control runtime system versions V3.5.16.0 and higher the "Users and Groups" page within the CODESYS Development System to configure the CODESYS Control runtime system's user management is a pure online editor. Every change to the editor will be transmitted immediately to the runtime system and there are no data kept within the CODESYS Development System. Because of this the *.dum file format to import or export the user management is not supported anymore for V3.5.16.0 CODESYS Control runtime systems. In contrast to this, the *.drm file format containing the user rights was not changed and the handling of this is as it was before.

• As replacement for the *.dum file, there is a new *.dum2 file, which is exported (created) and imported by the CODESYS Control runtime system itself. The user can trigger the generation and upload of the *.dum2 file by the CODESYS Development System to back up the user management configuration. For further protection, this file is optionally encrypted with a user chosen password. During download of the *.dum2 file, the password is requested by the CODESYS Control runtime system to restore the user management. The en-/decryption is handled on this device itself.

• With V3.5.16.0, the user group "Everyone" was removed from the runtime system. When importing an existing user management, this user group will be skipped from the old database. Because of this, imported groups may have less rights than before, if you did modify the CODESYS provided default groups or add own groups. In this case, you have to add the previously granted access rights of the group "Everyone" to all other groups. If you have multiple devices, you can export the updated database and roll out this new version to all other devices.

• CODESYS Data Source Manager: If the communication is based on the data source type CODESYS Application V3, there is at least the compiler version V3.5.16.0 necessary to support the new password transport protection by this client. Thus, existing projects require an update of the compiler version.

For device manufacturers we provide additional update information as part of the CODESYS Control V3 Runtime System Documentation here (registration required): https://customers.codesys.com/product-info/RTSOnlineHelp/Appendix/UserManagementUpdateInformation/index.html.

Update for CODESYS Control runtime systems V3.5.17.0

With V3.5.17.0 we enter the next level. As of this version, the online user management of the CODESYS Control runtime system is enforced by default.

Because of this, the user management must be activated, before clients can successfully log in to the CODESYS Control runtime. This applies to the CODESYS Development System and all other clients such as CODESYS HMI, PLCHandler, CODESYS OPC DA Server and OPC UA Clients. Activating the user management can be done by connecting with a CODESYS Development System (version must be at least V3.5.16.0). During the first connect, the user have to define an administrator user with own credentials.

We recommend using the administrator account only for administrative purposes, for example, to create additional users or to configure the online user management. For operational access to the CODESYS Control runtime system, additional users should be created and assigned to a group that only has the rights required for the respective job.

In case of updating a CODESYS Control runtime system, an existing user management is taken over, otherwise it is necessary to activate the user management.

In order to allow OPC UA clients still an anonymous login without needing to deactivate the user management completely, starting with V3.5.17.0 an anonymous access can be granted for OPC UA clients. In this case, the device user management remains active/enforced for all other clients.

To ensure that no attacker can hijack the controller directly after installation, the CODESYS Control runtime system should only be commissioned in a secure environment. This includes all stages from the installation of the CODESYS Control runtime system to the activation of the user management by creating the first administrator user.

Please find more information in the CODESYS V3.5.17.0 Online help, chapter Security: https://help.codesys.com/webapp/_cds_struct_security;product=codesys.

For device manufacturers we provide additional information on configuring the online user management in the CODESYS Control V3 Runtime System Documentation for V3.5.17.0, chapter "CODESYS Control - What's new".

Note: We recently introduced a new version scheme for the CODESYS Control SL runtime system products. The CODESYS Control V3 Runtime System Toolkit V3.5.17.0 will be the base of version V4.1.0.0 of these products.

5 Mitigation

3S-Smart Software Solutions GmbH strongly recommends using the available software update to fix the vulnerabilities.

In order to protect the CODESYS Control runtime system, the online user management has to be activated or preferably enforced if it has not yet been done. This not only prevents an attacker from downloading or executing malicious code, but also suppresses start, stop, debug, or other actions on a known working application that could potentially disrupt a machine or system.

To allow only trusted application code to be executed, the CODESYS Control runtime system also offers an advanced setting for device manufacturers to configure the code protection level for boot and downloaded applications. The SIGNED_AND_ENCRYPTED and MIN_SIGNED levels require that the CODESYS application has been signed with a valid and trusted X.509 user certificate.

In addition, or at least in the case that the software update is not applied, 3S-Smart Software Solutions GmbH recommends activating and using encryption of online communication whenever possible. The encrypted communication protects the password transmission by a TLS based encryption, independent of the weak password transmission affected by the vulnerabilities above.

Online communication encryption, online user management, and application code protection have been available for several service packs. For more information on enabling and enforcing encrypted communication and user management, see the CODESYS online help.

Furthermore, unauthorized local and all other remote access to the CODESYS control runtime system's file system must be prevented by additional means.

3S-Smart Software Solutions GmbH recommends as part of the mitigation strategy the following defensive measures to reduce the risk of exploitation of this vulnerability:

- Use controllers and devices only in a protected environment to minimize network exposure and ensure that they are not accessible from outside
- Use firewalls to protect and separate the control system network from other networks
- Use VPN (Virtual Private Networks) tunnels if remote access is required
- Activate and apply user management and password features
- Limit the access to both development and control system by physical means, operating system features, etc.
- Protect both development and control system by using up to date virus detecting solutions

For more information and general recommendations for protecting machines and plants, see also the CODESYS Security Whitepaper [1].

6 Acknowledgments

3S-Smart Software Solutions GmbH thanks those in the security community, who help us to improve our products and to protect customers and users through coordinated vulnerability disclosure.

We thank the following researchers for reporting these vulnerabilities independently from each other following coordinated disclosure:

• Nico Jansen from FH Aachen University of Applied Sciences

• Alexander Nochvay from Kaspersky Lab ICS CERT

• Martin Hartmann from cirosec GmbH

• Lab. of Information Systems Security Assurance (Kangbin Yim, Eunseon Jeong, Junyoung Park, Jeonghyeon Gim, Byeonggeun Son) in Soonchunhyang (SCH) University

• Carl Hurd of Cisco Talos

7 Further Information

For additional information regarding the CODESYS products, especially the above-mentioned versions, or about the described vulnerability please contact the 3S-Smart Software Solutions support team [5].

8 Disclaimer

Note: Not all CODESYS features are available in all territories. For more information on geographic restrictions, please contact sales@codesys.com.

Bibliography

[1] 3S-Smart Software Solutions GmbH: CODESYS Security Whitepaper
[2] 3S-Smart Software Solutions GmbH: Coordinated Disclosure Policy
[3] 3S-Smart Software Solutions GmbH CODESYS update area: https://www.codesys.com/download
[4] 3S-Smart Software Solutions GmbH security information page: https://www.codesys.com/security
[5] 3S-Smart Software Solutions GmbH support contact site: https://www.codesys.com/support
[6] Common Vulnerabilities and Exposures (CVE): https://cve.mitre.org
[7] CVSS Calculator: https://www.first.org/cvss/calculator/3.0
[8] ICS-CERT: https://ics-cert.us-cert.gov

The latest version of this document can be found here:

https://customers.codesys.com/index.php?eID=dumpFile&t=f&f=12943&token=d097958a67ba382de688916f77e3013c0802fade&download=

Change History

Version	Description	Date
1.0	First version	22.07.2019
2.0	Public reference added, release date of fix version updated	18.12.2019
3.0	New style sheet, complete update	24.04.2020
4.0	Software update available	06.05.2020
5.0	Further CVE added	12.05.2020
6.0	Link to device manufacturer documentation changed	16.06.2020
7.0	Online user management is now enabled by default: Additional JIRA reference CDS-73742 added, Available software updates extended by V3.5.17.0 update	29.03.2021